AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Digital Devices described in Attachment A,currently located at the Federal Bureau of Investigation (FBI), 9109 NE Cascades Parkway, Portland, Oregon 97220

Case No. '17-MC-658

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Digital devices described in Attachment A, incorporated by reference herein,

located in the _____ District of Oregon , there is now concealed *(identify the person or describe the property to be seized)*:

the information and items set forth in Attachment B, incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2252A(a)(1), (a)(5)(B)	Transportation and Possession of Child Pornography

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

TFO Celeste R. Fender, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: Dec. 13, 2017

Judge's signature

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF CELESTE R. FENDER

Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize Evidence Including Digital Evidence

I, Celeste R. Fender, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Detective employed by the Portland Police Bureau (PPB) and have been so employed since December 1997. I am also a Task Force Agent with the Federal Bureau of Investigation (FBI), and have been since September 2014. I am currently assigned to the Portland Division of the FBI where I investigate computer-related crimes. I have received training in the investigation of computer, telecommunications, and other technology crimes. Since September 2014, I have been involved in the investigation of matters involving the sexual exploitation of children, including the online sexual exploitation of children, particularly as it relates to violations of Title 18, United States Code (U.S.C.), Sections 2252A and 2422. I am part of the Portland Child Exploitation Task Force (CETF), which includes FBI Special Agents and a Hillsboro Police Department detective. CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer. As a member of this task force, I have received training in areas related to online computer crime investigation involving child pornography and other aspects of child exploitation.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of:

a) 1 (One) Seagate external hard drive Serial # NA8FQCEC;

b) 1 (One) Seagate external hard drive Serial # NA8FQCTN;

c) 1 (One)Seagate external hard drive Serial # NA4KVFKT;

d) 1 (One) Seagate external hard drive Serial # NA8EJ3W3;

e) 1 (One) Seagate external hard drive Serial # NA8EWDEG;

f) 1 (One) Seagate external hard drive Serial # NA8F25OR;

g) 1 (One) Sandisk (1GB) Micro SD card;

h) 1 (One) Sandisk (128GB) Micro SD card;

i) 1 (One) gray PNY (128GB) thumb drive;

j) 1 (One) Blue thumb drive with label "Essential Softwares"; and

k) 1 (One) Blue (4GB) thumb drive,

(hereinafter "Devices"), which are currently stored, in law enforcement possession, at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland, Oregon 97220, as described in Attachment A, incorporated herein by reference, and the extraction of electronically stored information from the Devices, as described in Attachment B, also incorporated by reference. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and (a)(5)(B) (Transportation and Possession of Child Pornography).

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation,

communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

4. 18 U.S.C. § 2252A(a)(1) makes it a crime to knowingly transport child pornography using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer.

5. 18 U.S.C. § 2252A(a)(5)(B) makes it a crime to knowingly possess material that contains an image of child pornography that has been shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. "Child pornography" is defined in 18 U.S.C. § 2256(8), and includes any visual depiction of a child under the age of 18 years engaged in sexually explicit conduct. "Sexually explicit conduct" is defined under 18 U.S.C. § 2256(2) and includes sexual intercourse, whether genital-genital, oral-genital, anal-genital, or oral-anal; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of the genitals or pubic area of any person.

Background on DC++

7. DC++ is an open source softward available to download from the internet for free. Utilizing the softward, users are able to conduct a search for specific items of interest. They are also able to connect directly with other users. All file transfers are made directly between users, not through the software.

Statement of Probable Cause

8. On December 5, 2017 at approximately 10:20 a.m. members of the HIDTA Interdiction Task Force (HIT) and Homeland Security Task Force Officers Randy Castaneda and Christopher Verbout were working criminal interdiction at the Amtrak station located at 800 NW 6th Avenue, Portland Oregon. As passengers exited the Amtrak train and walked towards the lobby area members of HIT consensually contacted passengers. All members of HIT were in plain clothes with no exterior police markings.

9. At about 10:20 a.m., Officer Verbout observed a person later identified as FONG LEE exit the sleeper car of Amtrak train #14. LEE was walking towards the terminal when Officer Verbout contacted him. Officer Verbout approached LEE from the side and did not impede his movements in any way. Officer Verbout was in plain clothes. Officer Verbout removed his Portland Police Bureau Badge from underneath his sweatshirt and showed it to LEE. Officer Verbout put his badge away and told LEE that he worked for the Portland Police Bureau and asked LEE if a K-9 could sniff his bag. LEE said, "Yes," and placed his black, gray and blue duffel bag on the concourse. Officer Verbout asked LEE if he would mind removing his backpack so the K-9 could sniff that as well. LEE said he did not mind and removed the backpack and placed it onto the concourse. Officer Scott Groshong then approached and utilized his K-9 partner "Rex" to conduct a sniff on the duffel bag and backpack. While Officer Groshong's K-9 was conducting his sniff, Officer Verbout asked LEE if he could look in the bags to make sure LEE did not have anything he was not supposed to have. LEE

said, "Sure, go ahead." Officer Verbout located a large quantity of US currency in LEE's bag.

10. LEE was asked if he was willing to accompany officers to an office to talk further. LEE agreed and went with officers to a police office located within the Amtrak station. LEE was advised of his rights per Miranda to which he stated he understood by responding, "Yes," at 10:33 a.m. Officers continued to speak with LEE and his companion, who was separately approached by another officer and also agreed to accompany him to the police office at the Amtrak station after officers discovered a large amount of currency in his bag as well. LEE and his companion admitted during the interview that they were traveling from Minnesota to California to purchase drugs (marijuana) with the cash they were carrying. LEE's companion stated that the money was his, that it was proceeds of prior drug sales, and he intended to transport the marijuana to Minnesota and re-sell it. The cash they were carrying totaled approximately $70,000.00.

11. Officer Verbout noticed that there were multiple external storage devices, USB drives, and Micro SD cards in LEE's belongings. Officer Verbout asked LEE what was in the digital media. LEE stated all of the devices belonged to him and nobody else had downloaded anything to any of the storage devices. LEE stated the devices contained art, drawings and "stuff." Officer Verbout asked LEE what was "Stuff." LEE stated the devices contained "Porn." Officer Verbout asked if the devices contained child pornography. LEE said, "Yes." Officer Verbout asked LEE if the devices contained young child pornography with six or seven year old kids. LEE

replied, "Yeah. I'm not going to lie to you. They do." Officer Verbout asked LEE if he was making any of the child pornography. LEE stated that he was not.

12. Based on the above, LEE and his companion were arrested and transported to PPB's Central Precinct Drugs and Vice Division office and placed in a holding cell. When there, Officer Verbout asked LEE if he would consent to a search of all the digital devices in his bag and backpack, as well as his cellular telephone. LEE agreed and signed a consent form.

13. FBI Task Force Officer (TFO) Cheryl Banks and Special Agent (SA) Rebecka Brown responded to PPB's Central Precinct, along with Northwest Regional Computer Forensics Laboratory's Forensic Examiners Kent Hughes and Justin Lazenby. Officer Verbout confirmed with LEE that anyone PPB designated could search all of the digital devices found in LEE's bag and backpack and his cell phone. LEE agreed and initialed the consent form, and the time was added to the form. The electronic devices were then provided to the Forensic Examiners for review.

Interview of Fong Lee

14. TFO Banks and SA Brown along with Officer Verbout interviewed LEE in an interview room on the 14th floor of the Central Precinct. Lee had previously been placed in handcuffs and the handcuffs remained in place throughout the interview. Lee was advised of the identities of TFO Banks and SA Brown. The interview was audio recorded and Lee was aware of the recording. Lee had previously been advised of his Miranda Rights by Officer Verbout and had stated he understood his Rights and agreed to answer questions. LEE agreed to talk to TFO Banks and SA Brown as well.

15. Lee admitted the digital devices seized by the Portland Police Bureau belonged to

him. He stated the devices would contain videos, pornography of all sorts, including child pornography. Lee further stated he used the Peer to Peer (P2P) program DC++, which is similar to BitTorrent and Limewire. Lee explained that a user of DC++ can conduct a search (similar to a Google search) using search terms such as "r@ygold", or "preteen". Lee stated he had heard of the term "PTHC" but did not know what it stood for (preteen hard core). Lee further explained he was able to download images and videos from DC++ without having to share images and videos. Lee stated if he shared an image or video, it was most likely non-pornographic in nature.

16. Lee was asked to describe what "child pornography" was and he stated it was "under 18" years of age and "doing anything sexual." Lee stated he has seen images and videos of child pornography depicting children around the age of 5 years. Lee admitted to downloading images and videos from DC++ and placing them on at least two of the hard drives in a folder titled "P".

17. Lee admitted to looking at images and videos of child pornography for about ten years and said he first discovered it by "messing around on the Internet." Lee stated there could possibly be upwards of 1,000 images and videos of child pornography located on his devices. Lee was asked why he travelled with the devices and he stated he could always purchase a new computer. Lee said he began to download images and videos of child pornography about five years ago when he lived in California. He said he then moved back and forth from California to Minnesota, and most likely took his collections with him.

18. Lee stated he knew that downloading and possessing images and videos of child

pornography was "illegal" but age didn't matter to him. It was Lee's opinion, based on his culture that an adult could have a sexual relationship with a child as long as the child wasn't "too young." Lee stated below 10 or 5 years would be considered too young. Lee admitted to having a sexual relationship with his 12-year-old sister when he was 21 years of age and living in California.

19. Lee denied producing images and videos of child pornography and when advised that a Search Warrant would be applied for and if granted, his devices would be fully examined by a forensics laboratory, Lee maintained no evidence of production of child pornography would be located.

Additional Information

20. Lee stated he was born in Laos, but grew up in the United States. He spoke fluent English and showed no signs of any language barrier.

21. Lee was later advised he was being arrested for Transportation and Possession of Child Pornography and he stated, "It doesn't matter."

22. PPB seized a ticket confirming that Lee was traveling from Minnesota to California when he got off the Amtrak train in Portland, Oregon, carrying the Devices described above and in Attachment A.

23. The Devices are currently in secure evidence storage at the FBI, 9109 NE Cascades Parkway, Portland, Oregon 97220. In my training and experience, I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Portland Police Bureau.

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Storage medium.* A storage medium is any physical object upon which computer data can be recorded. Examples include external hard drives, RAM, floppy disks, thumb drives, flash memory, CD-ROMs, Micro SD cards and other magnetic or optical media.

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten.

26. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Device because, based on my knowledge, training, and experience, I know:

a. The process of identifying the exact electronically stored information on a

storage medium necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

b. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire mediums, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

28. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of

the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

29. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or images do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

30. If an examination is conducted, and it is determined that any of the Devices do not contain any data falling within the ambit of the warrant, the government will return such Devices to the owner within a reasonable period of time following the search and will seal any image of such Device(s), absent further authorization from the Court.

31. The government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime, or to commence forfeiture proceedings against the Devices and/or the data contained therein.

32. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

33. *Manner of execution.* Because this warrant seeks only permission to examine Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

34. Based on the foregoing, I have probable cause to believe, and I do believe, that the Devices described in Attachment A, contain evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(1) and (a)(5)(B), as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Devices described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

35. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Jane Shoemaker, and AUSA Jane Shoemaker advised me that in her opinion the affidavit and application are legally and factually sufficient to establish probable cause to

///

///

///

///

///

///

///

support the issuance of the requested warrant.

TFO CELESTE R. FENDER
Federal Bureau of Investigation

Subscribed and sworn to before me this 13th day of December 2017.

STACIE F. BECKERMAN
United States Magistrate Judge

ATTACHMENT A

ATTACHMENT A

Items to be Searched

1. The following digital devices, which were seized from Fong Lee, DOB XX-XX-1985, on or about December 5, 2017, and are currently in secure evidence storage at the Federal Bureau of Investigation, 9109 NE Cascades Parkway, Portland, Oregon 97220:

a) 1 (One) Seagate external hard drive Serial # NA8FQCEC

b) 1 (One) Seagate external hard drive Serial # NA8FQCTN

c) 1 (One)Seagate external hard drive Serial # NA4KVFKT

d) 1 (One) Seagate external hard drive Serial # NA8EJ3W3

e) 1 (One) Seagate external hard drive Serial # NA8EWDEG

f) 1 (One) Seagate external hard drive Serial # NA8F25OR

g) 1 (One) Sandisk (1GB) Micro SD card

h) 1 (One) Sandisk (128GB) Micro SD card

i) 1 (One) gray PNY (128GB) thumb drive

j) 1 (One) Blue thumb drive with label "Essential Softwares"

k) 1 (One) Blue (4GB) thumb drive

ATTACHMENT B

ATTACHMENT B

Items to Be Seized

1. The items to be searched for, seized, and examined, are all items that constitute or contain evidence, contraband, fruits, and/or instrumentalities of violations of Title 18, United States Code, Section 2252A(a)(2) (Distribution of Child Pornography) and 2252A(a)(5)(B) (Knowing Possession of Child Pornography), including:

a. All visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, including all motion pictures or digital video clips containing such visual depictions;

b. All video recordings which are self-produced and pertain to sexually explicit images of minors, or video recordings of minors which may assist in the location of minor victims of child exploitation or child abuse;

c. All records and information, including written or electronic correspondence or communications, pertaining to the production, transportation, shipment, distribution, receipt, trade, sale, purchase, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 USC 2256, or any attempt to commit any such offense;

d. All records or information that pertain to offers to transmit, the solicitation of a transmission, or the transmission, through interstate or foreign commerce by any means (including by computer), of any visual depiction of a minor engaged in sexually explicit conduct, as defined in 18 USC 2256;

e. All records or information naming or identifying minors visually depicted while engaging in sexually explicit conduct, as defined in 18 USC 2256;

f. Any records of Internet usage, including records containing screen names, user names, and e-mail addresses, and identities assumed for the purposes of communication on the Internet. These records include electronic files on data storage media, including external hard drives, thumb drives, and SD cards;

g. All records or information referring or pertaining to communications with others, whether in person, by telephone, or online, for the purpose of producing, distributing, transporting, receiving, or possessing child pornography as defined in 18 USC 2256, including chat logs, call logs, address books or contact list entries, digital images sent or received, and the like;

h. All images and video clips of child erotica, defined as material or items that may be sexually arousing to persons having a sexual interest in children but that are not in and of themselves legally obscene and do not depict minors engaged in sexually explicit conduct as defined in 18 USC 2256, such as images of minors depicted in underwear or partially undressed; and

i. Storage media used as a means to commit or facilitate the violations described above.

2. As used in this attachment, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. The term "computer" includes all

types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include flash memory and other magnetic or optical media.

3. For any storage medium whose seizure is otherwise authorized by this warrant and any storage medium that contains or in which is stored records or information that is otherwise called for by this warrant ("Device"):

a. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as documents, photographs, and correspondence.

b. Evidence of software that would allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence indicating how and when the Devices were accessed or used to determine the chronological context of Device access, use, and events relating to the crimes under investigation and to the Device user.

d. Evidence of the attachment of the Devices to a computer.

e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Devices.

f. Evidence of the dates and times the Devices were used.

g. Passwords, encryption keys, and other access devices that may be

necessary to access the Devices.

h. Contextual information necessary to understand the evidence described in this attachment.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device, may require authorities to employ techniques, including imaging storage media and computer-assisted scans and searches of the storage media, that might expose many parts of the storage media to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted, and the storage media do not contain any data falling within the ambit of the warrant, the government will return the storage media to its owner within a reasonable period of time following the search and will seal any image of the storage media, absent further authorization from the Court.

8. The government may retain the storage media as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the storage media and/or the data contained therein if evidence falling within the ambit of the warrant is found.

9. The government will retain a forensic image of the storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.